Kim D. Stephens, OSB #030635
Cecily C. Jordan (*Pro Hac Vice* forthcoming)
Kaleigh N. Boyd (*Pro Hac Vice* forthcoming)
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600

Daniel O. Herrera (*Pro Hac Vice* forthcoming)
Nickolas J. Hagman (*Pro Hac Vice* forthcoming)
Mohammed A. Rathur ((*Pro Hac Vice* forthcoming)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485

Additional attorney signature blocks listed below.

Attorneys for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

(PORTLAND DIVISION)

LISA UNSWORTH, MICHAEL RAMONE, CHRISTOPHER POTTER, THERESE COOPER, and CHARLES SANDERSON, individually, and on behalf of all others similarly situated, Plaintiffs, v. LEWIS AND CLARK COLLEGE, Defendant.	Case No. 3:24-cv-00614-SB AMENDED CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Lisa Unsworth, Michael Ramone, Christopher Potter, Therese Cooper, and Charles Sanderson, ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Lewis and Clark College ("Lewis and Clark" or "Defendant"), by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Lewis and Clark is a private college based in Portland, Oregon that consists of one undergraduate program—the College of Arts and Sciences—and two graduate programs—the Graduate School of Education and Counseling, and the School of Law.[1]

2. As part of its operations Lewis and Clark collects, maintains, and stores highly sensitive personal information and protected health information pertaining Lewis and Clark's current and former students and employees, including, but not limited to their names, dates of birth, Social Security numbers, driver's license or state identification numbers, passports (collectively, personally identifiable information or "PII"), medical information and health insurance information (collectively, protected health information or "PHI"), and financial account numbers and financial account routing numbers (collectively, with PII and PHI, "Private Information").[2]

3. On or about February 28, 2023, Lewis and Clark experienced a data security incident where unauthorized cybercriminals accessed Lewis and Clark's information systems and databases (the "Data Breach"). Lewis and Clark discovered this unauthorized access on March 3,

[1] *See* https://www.lclark.edu/about/ (last accessed April 4, 2024).

[2] *See Lewis & Clark Notifies Individuals of Data Security Incident*, Lewis & Clark

2023, and launched an investigation with the aid of third-party data security specialists. In February 2024, Lewis and Clark determined that unauthorized actors were able to access and exfiltrate Private Information concerning Plaintiffs' and Class members.

4. In April 2024, Lewis and Clark sent notices to individuals whose information was accessed in the Data Breach.

5. Because Lewis and Clark stored and handled such highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Lewis and Clark failed to fulfill these obligations, as unauthorized cybercriminals breached Lewis and Clark's information systems and databases and stole vast quantities of Private Information belonging to Plaintiffs and Class members. The Data Breach and the successful exfiltration of Private Information were the direct, proximate, and foreseeable results of multiple failings on the part of Lewis and Clark.

7. The Data Breach occurred because Lewis and Clark inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, Lewis and Clark failed to timely detect this Data Breach until almost an entire year after the Data Breach occurred. Prior to the Data Breach, Lewis and Clark failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been made aware of this fact, they would have never provided their Private Information to Defendant.

8. Lewis and Clark's meager attempt to ameliorate the effects of this Data Breach with one year of complimentary credit monitoring is woefully inadequate. Much of the Private

Information that was stolen is immutable and one year of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

9. As a result of Lewis and Clark's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class members suffered injuries including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiffs' and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Lisa Unsworth

11. Plaintiff Lisa Unsworth is a resident of Cathlamet, Washington. Plaintiff Unsworth was an employee of Lewis and Clark from 2005 to 2009, and she received Lewis and Clark's Data Breach Notice.

Plaintiff Dr. Michael Ramone

12. Plaintiff Dr. Michael Ramone is a resident of Portland, Oregon. Plaintiff Ramone graduated from Lewis and Clark Law School in 2003, and he received Lewis and Clark's Data Breach Notice.

Plaintiff Christopher Potter

13. Plaintiff Christopher Potter is a resident of Oregon. Plaintiff Potter is an employee of Lewis and Clark, and he received Lewis and Clark's Data Breach Notice.

Plaintiff Therese Cooper

14. Plaintiff Therese Cooper is a resident of Portland, Oregon. Plaintiff Cooper was student at Lewis and Clark for years, ending in the Spring of 2012, and she received Lewis and Clark's Data Breach Notice.

Plaintiff Charles Sanderson

15. Plaintiff Charles Sanderson is a resident of Portland, Oregon. Plaintiff is a former student at Lewis and Clark College. He received a notice of the Data Breach from the Defendant in April 2024.

Defendant Lewis and Clark

16. Defendant Lewis and Clark is an entity incorporated under the laws of the State of Oregon with its principal place of business at 615 South Palatine Hill Road Portland, Oregon, 97219.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Lewis and Clark. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Lewis and Clark because Lewis and Clark is headquartered in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District and because Lewis and Clark resides in this District.

IV. FACTUAL ALLEGATIONS

A. Lewis and Clark – Background

20. Lewis and Clark is a private college based in Portland that offers an undergraduate program and two graduate programs.

21. As part of its normal operations, Defendant collects, maintains, and stores the highly sensitive Private Information provided by its current and former employees and students, including but not limited their names, dates of birth, Social Security numbers, driver's license or state identification numbers, passports, medical information and health insurance information, and financial account numbers and financial account routing numbers.

22. Current and former students of Defendant made their Private Information available to Lewis and Clark with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and

unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

23. This expectation was a objectively reasonable and based on an obligation imposed on Lewis and Clark by statute, regulations, industrial custom, and standards of general due care.

24. Unfortunately for Plaintiffs and Class members, Lewis and Clark failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

25. According to Lewis and Clark's public statements, cybercriminals breached its information systems and databases on or about February 28, 2023. Lewis and Clark discovered the Data Breach on March 3, 2023.

26. On February 24, 2024, Lewis and Clark determined that its current and former employees' and students' Private Information was exfiltrated.

27. On April 3, 2024— more than ***one year*** after the Lewis and Clark discovered the unauthorized access to its data systems—Lewis and Clark sent notice of the Data Breach to all individuals affected by the Data Breach.

C. Lewis and Clark's Many Failures Both Prior to and Following the Breach

28. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiffs and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

29. First, Defendant failed to implement reasonable security protections to safeguard its information systems and databases.

30. Second, Defendant failed to timely detect this Data Breach with Defendant only becoming aware of the intrusion almost an entire year after the unauthorized actors gained access to Defendant's systems. This delayed detection gave these cybercriminals with an entire year to access, peruse, steal, and exploit the sensitive Private Information of Defendant's employees and students.

31. Third, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant.

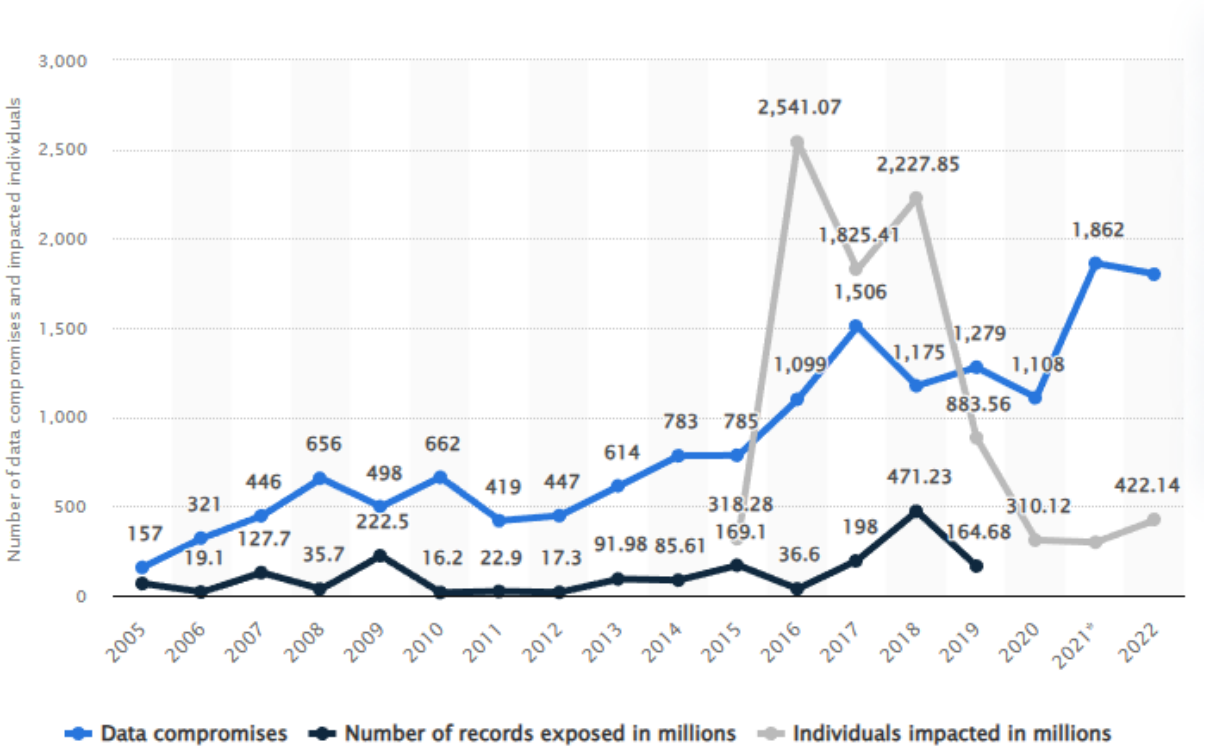
32. Additionally, Defendant's attempt to ameliorate the effects of this Data Breach with one year of complimentary credit monitoring is woefully inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as a Social Security number, is immutable.

33. In short, Defendant's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their personal and financial information had been stolen due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information for nearly a year before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

34. Data Breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that Private Information, Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. Statista, a German entity that collects and markets data relating to, among other things, Data Breach incidents and the consequences thereof, confirms that the number of Data Breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[3] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[4]



[3] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[4] *Id.*

36. This stolen Private Information is then routinely traded on dark web black markets as s simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[5]

37. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

38. This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[7]

---

[5] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

[6] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[7] *Id.*

39. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases conc against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard personal information.[8]

40. Given the nature of Defendant's Data Breach, as well as the length of the time Defendant's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

41. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer Data Breach, because credit card victims can cancel or close credit and debit card accounts.[9] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

42. To date, Defendant has offered its consumers only 12 months of identity theft monitoring services. The offered services are inadequate to protect Plaintiffs and the Class from

[8] *See e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).
[9] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

the threats they will face for years to come, particularly in light of the Private Information at issue here.

43. Despite the prevalence of public announcements of Data Breach and data security compromises, its own acknowledgment of the risks posed by Data Breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former employees.

E. Lewis and Clark Had a Duty and Obligation to Protect Private Information

44. Defendant has an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including FTC and various state's rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive Private Information. Plaintiffs and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. FTC Act Requirements and Violations

45. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[10] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[11] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

47. The FTC further recommends that companies not maintain personally identifying information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[11] *Id.*
[12] *Id.*

unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

50. Defendant was fully aware of its obligation to protect the Private Information of its current and former employees, including Plaintiffs and the Class, and on information and belief, Defendant is a sophisticated and technologically savvy entity that relies extensively on technology systems and networks to maintain its practice, including storing its employees' Private Information in order to operate its business.

51. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a Data Breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

2. Industry Standards and Noncompliance

52. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

53. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information like Defendant include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and

anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

54. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

55. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

56. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

57. Like any data hack, the Data Breach presents major problems for all affected.[13]

58. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC

[13] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last accessed August 12, 2023).

notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[14]

59. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

60. According to data security experts, one out of every four Data Breach notification recipients become a victim of identity fraud.

61. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

62. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports", public and corporate Data Breaches correlate to an increased risk of identity theft for victimized consumers.[15] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[16]

[14] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.
[15] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[16] *Id.*

63. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

64. Data Breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[17]

65. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with just 12 months of credit monitoring through Cyber Scout. However, this is much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendant's failures.

66. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

67. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and

[17] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRINbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.

identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

68. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within a mere 12 months: the unauthorized access of Plaintiffs and Class members' Private Information, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach.

69. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

70. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFFS

Lisa Unsworth

71. Plaintiff Lisa Unsworth was an employee of Lewis and Clark from 2005 to 2009.

72. As a condition of her employment, Plaintiff Unsworth was required to provide Defendant with her Private Information.

73. In April 2024, Plaintiff Unsworth received Lewis and Clark's Data Breach notice. The notice informed Plaintiff Unsworth that her Private Information was improperly accessed and obtained by third parties, including but not limited to Plaintiff's Social Security number, financial account number, financial account routing number, and health insurance information.

74. After the Data Breach, Plaintiff Unsworth experienced a dramatic increase in the number of spam phone calls, text messages, and emails.

75. As a result of the Data Breach and the resulting suspicious activity, Plaintiff Unsworth made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

76. As a result of the Data Breach, Plaintiff Unsworth suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Unsworth is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

77. Plaintiff Unsworth suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained

from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

78. As a result of the Data Breach, Plaintiff Unsworth anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Dr. Michael Ramone

79. Plaintiff Dr. Michael Ramone graduated from Lewis and Clark Law School in 2003.

80. As a condition of his enrollment, Plaintiff Ramone was required to provide Defendant with his Private Information.

81. In April 2024, Plaintiff Ramone received Lewis and Clark's Data Breach notice. The notice informed Plaintiff Ramone that his Private Information was improperly accessed and obtained by third parties, including but not limited to his Social Security number and health insurance information.

82. After the Data Breach, Plaintiff Ramone had his Android tablet hacked into by an unknown third party.

83. As a result of the Data Breach and the resulting suspicious activity, Plaintiff Ramone made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach. He has also spent time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

84. As a result of the Data Breach, Plaintiff Ramone suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff Ramone is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

85. Plaintiff Ramone suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

86. As a result of the Data Breach, Plaintiff Ramone anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Christopher Potter

87. Plaintiff Christopher Potter is a current employee of Lewis and Clark.

88. As a condition of his employment, Plaintiff Potter was required to provide Defendant with his Private Information.

89. In April 2024, Plaintiff Potter received Lewis and Clark's Data Breach notice. The notice informed Plaintiff Potter that his Private Information was improperly accessed and obtained by third parties, including but not limited to his Social Security number and health insurance information.

90. As a result of the Data Breach, Plaintiff Potter made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and monitoring his financial accounts for suspicious activity. He has also spent time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

91. As a result of the Data Breach, Plaintiff Potter suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his private information for purposes of identity theft and fraud. Plaintiff Potter is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

92. Plaintiff Potter suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

93. As a result of the Data Breach, Plaintiff Potter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Therese Cooper

94. Plaintiff Therese Cooper was a student at Lewis and Clark for years, ending in the Spring of 2012.

95. As a condition of her enrollment, Plaintiff Cooper was required to provide Defendant with her Private Information.

96. In April 2024, Plaintiff Cooper received Lewis and Clark's Data Breach notice. The notice informed Plaintiff Cooper that her Private Information was improperly accessed and obtained by third parties, including but not limited to Plaintiff's Social Security number, financial account number, financial account routing number, and health insurance information.

97. As a result of the Data Breach, Plaintiff Cooper made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

98. As a result of the Data Breach, Plaintiff Cooper suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Cooper is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. Plaintiff Cooper suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

100. As a result of the Data Breach, Plaintiff Cooper anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Charles Sanderson

101. Plaintiff Sanderson is a former student of Lewis and Clark College.

102. As a condition of enrollment, Plaintiff was required to provide Defendant with their Private Information.

103. In April 2024, Plaintiff Sanderson received Lewis and Clark's Data Breach notice. The notice informed Plaintiff that his private information was improperly accessed and obtained by third parties, including but not limited to his Social Security number, financial account information and his health insurance information.

104. As a consequence of the Data Breach, Plaintiff Sanderson undertook reasonable efforts to mitigate its effects. These efforts included, but were not limited to, researching the breach, and meticulously reviewing credit reports and financial account statements for signs of actual or attempted identity theft or fraud. He has also dedicated several hours to addressing the breach, time that he would have otherwise allocated to other activities, such as work and recreation.

105. As a result of the Data Breach, Plaintiff Sanderson experienced anxiety due to the public exposure of his personal information, which he believed would be safeguarded against unauthorized access and disclosure. His anxiety is primarily driven by concerns about unauthorized parties viewing, selling, and using her private information for identity theft and fraud. Plaintiff Sanderson is especially troubled by the potential for identity theft and fraud, as well as the resulting consequences from the Data Breach.

106. As a consequence of the Data Breach, Plaintiff Sanderson expects to invest significant time and money continuously to mitigate and address the resulting harms. Furthermore, he currently faces an increased risk of identity theft and fraud, a risk that is likely to persist for years to come.

107. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

108. Since the Data Breach, Plaintiff has endured a substantial uptick in spam phone calls and targeted phishing attempts on his email and personal phone number. Plaintiff asserts that these incidents are directly and causally linked to the timeline of the Data Breach

109. Plaintiff Sanderson has a continuing and legitimate interest in ensuring that his Private Information is protected and safeguarded from future breaches.

V. CLASS REPRESENTATION ALLEGATIONS

110. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

111. In the alternative, Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Oregon whose Private Information was accessed in the Data Breach (the "Oregon Subclass").

Excluded from the Oregon Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

112. In the alternative, Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Washington whose Private Information was accessed in the Data Breach (the "Washington Subclass").

Excluded from the Washington Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

113. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process, but, on information and belief, consist of tens of thousands of individuals. The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

114. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant owed a duty to Class members to safeguard their Private Information;

h. Whether Defendant breached its duty to Class members to safeguard their Private Information;

i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

k. Whether Defendant's conduct violated the FTCA, and/or the Consumer Protection Act invoked herein;

l. Whether Defendant's conduct was negligent;

m. Whether Defendant's conduct was *per se* negligent;

n. Whether Defendant was unjustly enriched;

o. What damages Plaintiffs and Class members suffered as a result of Defendant's misconduct;

p. Whether Plaintiffs and Class members are entitled to actual damages;

q. Whether Plaintiffs and Class members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

115. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

116. Adequacy: Plaintiffs are adequate class representatives because Plaintiffs' interests do not materially or irreconcilably conflict with the interests of the Class Plaintiffs seek to represent, Plaintiffs retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute their action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

117. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast,

the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiffs on behalf of the Class)

118. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

119. Defendant owes a duty of care to protect the Private Information belonging to Plaintiffs and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a Data Breach and to timely act on warnings about Data Breaches; and

f. to promptly notify Plaintiffs and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

120. Defendant also owes them a duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Defendant to use reasonable measures to protect confidential data.

121. Defendant also owes them duty because industry standards mandate that Defendant protect its employees' confidential Private Information.

122. Defendant also owes them a duty because it had a special relationship with Plaintiffs' and Class members. Plaintiffs and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect their information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

123. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiffs and the Class. Their duty exists to allow Plaintiffs and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

124. Defendant breached its duties to Plaintiffs and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiffs and Class members.

125. Defendant also breached the duties it owed to Plaintiffs and the Class by failing to timely and accurately disclose to Plaintiffs and Class members that their Private Information had been improperly acquired and/or accessed.

126. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of

time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

- Permanent increased risk of identity theft.

127. Plaintiffs and Class members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

128. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiffs and Class members.

129. Plaintiffs are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiffs on behalf of the Class)

130. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

131. Section 5 of the FTCA imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class members.

132. Defendant violated the FTCA and state rules and regulations by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class members' Private Information.

133. Defendant's failure to comply with the FTCA and applicable state rules and regulations constitutes negligence *per se*.

134. Plaintiffs and Class members are within the class of persons that the FTCA and state rules and regulations are intended to protect.

135. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

136. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

137. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiffs on behalf of the Class)

138. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

139. Plaintiffs and the Class provided Defendant with their Private Information.

140. By providing their Private Information, and upon Defendant's acceptance of their information, Plaintiffs and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

141. The implied contracts between Defendant and Plaintiffs and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

142. The implied contracts for data security also obligated Defendant to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

143. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiffs and Class members; allowing unauthorized persons to access Plaintiffs' and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class members, as alleged above.

144. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Class)

145. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

146. This count is brought in the alternative to Count III.

147. Plaintiffs and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

148. Defendant was benefitted by the conferral upon it of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

149. Defendant also understood and appreciated that Plaintiffs' and Class members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

150. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining students, gaining the reputational advantages conferred upon it by Plaintiffs and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

151. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private

Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

152. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

153. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

154. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

155. Defendant is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the PII that was accessed in the Data Breach and the profits Defendant receives from the use and sale of that information.

156. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

157. Plaintiffs and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
INTRUSION UPON SECLUSION
(By Plaintiffs on behalf of the Class)

158. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

159. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

160. By failing to keep Plaintiffs' and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

161. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendant's actions highly offensive.

162. Defendant invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

163. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

164. In failing to protect Plaintiffs' and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiffs' and Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its thousands of students. Plaintiffs, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT VI
VIOLATIONS OF OREGON UNLAWFUL TRADE PRACTICES ACT
(On Behalf of Plaintiffs and the Class)

165. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

166. Plaintiffs are authorized to bring this claim under Or. Rev. Stat. § 646.638(1).

167. Or. Rev. Stat. § 646.608(1), *et seq*. ("OUTPA"), prohibits "unlawful practice[]s in the course of the person's business, vocation or occupation . . . ." Or. Rev. Stat. § 646.608(1).

168. As described in this Complaint, Defendant has engaged in the following unfair or deceptive acts or practices in violation of the OUTPA:

> (e) Represent[ing] that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that the real estate, goods, or services do not have or that a person has a sponsorship, approval, status, qualification, affiliation, or connection that the person does not have;
>
> (g) Represent[ing] that real estate, goods or services are of a particular standard, quality, or grade, or that real estate or goods are of a particular style or model, if the real estate, goods or services are of another; and
>
> (u) Engag[ing] in any other unfair or deceptive conduct in trade or commerce.

Or. Rev. Stat. §§ 646.608(e), (g), (u).

169. Defendant's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

170. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services to consumers throughout the United States.

171. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiffs' and Class members' Private Information and other Defendant data was vulnerable.

172. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

173. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

174. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices and regarding the security of the sensitive Private Information. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiffs' and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiffs, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former students' and employees' Private Information and other records.

175. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

176. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiffs' and Class members' Private Information.

177. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former students' and employees' Private Information.

178. Had Defendant disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

179. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

180. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws such as the FTC Act.

181. The injuries suffered by Plaintiffs and the Class greatly outweigh any potential countervailing benefit to consumers or to competition and are not injuries that Plaintiffs and the Class should have reasonably avoided.

182. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and the Class as a direct result of Defendant's deceptive acts and

practices as set forth herein include, without limitation: (i) Plaintiffs experiencing an increase in spam calls, texts, and/or emails; (ii) invasion of privacy; (iii) theft of their Private Information; (vi) lost or diminished value of Private Information; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its students' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

183. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VII
VIOLATIONS OF WASHINGTON CONSUMER PROTECTION ACT
(On Behalf of Plaintiff Unsworth and the Washington Subclass)

184. Plaintiff Lisa Unsworth ("Plaintiff," for the purposes of this Count) restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

185. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

186. Defendant is a "person" as described in RCW 19.86.010(1).

187. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

188. In the course of conducting its business, Defendant committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' Private Information. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

189. Defendant's above-described "unfair or deceptive acts or practices" affects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

190. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

191. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff and Class members' business and property. Plaintiff and Class members have suffered, and will continue to suffer, actual damages and injury in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or

her Private Information; (5) deprivation of the value of his or her Private Information, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them.

192. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect Private Information.

193. Plaintiff, on behalf of herself and the Class, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff, on behalf of herself and the Class, requests that this Court use its discretion under RCW 19.86.090 to increase the damages award for each class member to three times the actual damages sustained, not to exceed $25,000.00 per class member.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

C. That the Court award Plaintiffs and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

D. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

E. That the Court award pre- and post-judgment interest at the maximum legal rate;

F. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

G. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Respectfully submitted this 28th day of June, 2024

TOUSELEY BRAIN STEPHENS PLLC

s/ Kim D. Stephens, P.S.
Kim D. Stephens, P.S., OSB #030635
Cecily C. Jordan*
Kaleigh N. Boyd*
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: (206) 682-5600
Facsimile: (206) 628-2992
kstephens@tousley.com
cjordan@tousley.com
kboyd@tousley.com

Daniel O. Herrera*
Nickolas J. Hagman*
Mohammed A. Rathur*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
mrathur@caffertyclobes.com

Philip Krzeski *
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
pkrzeski@chestnutcambronne.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiffs and the Proposed Class